Akamai-Kundenreferenz

Führendes Werbeunternehmen setzt auf Zero Trust

Das Unternehmen qualifizierte sich für eine Cyberversicherung, verhinderte Angriffe und konnte geistiges Eigentum durch Mikrosegmentierung besser schützen

Cyberversicherung erhalten | Bedrohungen erkannt | Angriffe verhindert

Marken den TV-Zuschauern näherbringen

Ein weltweit führender Anbieter von vernetzter TV-Werbung unterstützt Marken dabei, ihre Werbeausgaben bestmöglich einzusetzen, indem sie das fragmentierte Streaming-Publikum besser erreichen. Als sich das Unternehmen für eine Cyberversicherung qualifizieren wollte, setzte es Akamai Guardicore Segmentation ein, um seine Sicherheitsmaßnahmen zu stärken.

Anspruch auf eine Cyberversicherung

Als innovative Firma legt das Unternehmen verständlicherweise Wert darauf, sein geistiges Eigentum (Intellectual Property, IP) zu schützen. Wie bei vielen modernen Unternehmen war das geistige Eigentum anfällig, sollte ein Bot oder Hacker die internen Server und Apps erfolgreich infiltrieren.

Um die finanziellen Auswirkungen eines möglichen Sicherheitsverstoßes zu begrenzen, forderte die Muttergesellschaft die IT-Abteilung auf, eine Cyberversicherung abzuschließen. Angesichts der zunehmenden Zahl von Cyberangriffen prüfen die Versicherer die Sicherheitsmaßnahmen der Unternehmen, bevor sie ihnen eine Police anbieten. Vor diesem Hintergrund entschied sich das Unternehmen für den Einsatz interner Segmentierung.

Advertising Leader

Standort

USA

Branche

Medien- und Unterhaltungsbranche

Lösung

Akamai Guardicore Segmentation

Einsatz interner Segmentierungskontrollen

Das Unternehmen hat seine Lösung mit Akamai Guardicore Segmentation gefunden, was einen softwarebasierten Ansatz für Mikrosegmentierung bietet. Akamai Guardicore Segmentation ist eine wichtige Komponente zum Schutz des geistigen Eigentums des Unternehmens und wurde entwickelt, um laterale Netzwerkbewegungen in der digitalen Umgebung durch Angreifer zu verhindern. Durch die Mikrosegmentierung kann das Unternehmen sicherstellen, dass die Server und Anwendungen – und deren Workloads –, die sein geistiges Eigentum enthalten, vollständig von der übrigen Infrastruktur getrennt sind.

Durch die Verwendung der Akamai Guardicore Segmentation zur Abschirmung kritischer Assets und zur Begrenzung lateraler Netzwerkbewegungen kann das Unternehmen sicherstellen, dass Angreifer sich nicht einfach in der gesamten IT-Umgebung bewegen können. Dank granularer Transparenz der Bewegungen innerhalb der physischen und virtuellen Umgebung können Angreifer einfacher aufgehalten werden.

Erkennung und Verhinderung von Ransomware-Angriffen

Um zu bestätigen, dass die Akamai Guardicore Segmentation die beste Option ist, führte das Unternehmen einen Machbarkeitsnachweis (Proof of Concept, PoC) durch. Während des PoC erkannte die Lösung von Akamai viele Angreifer und sogar einen Ransomware-Vorfall.

Nachdem das Unternehmen die Vorteile von Akamai Guardicore Segmentation zum Schutz seiner Umgebung erkannt hatte, wusste es, dass es die richtige Lösung gefunden hatte. Das Unternehmen plant, mehr als 3.000 Server – eine Mischung aus Linux-, Bare-Metal- und Cloudservern – und etwa 1.500 Container (Docker und Kubernetes) zu segmentieren.

| Veröffentlicht: November 2024